In the Specification:

Please amend the paragraph on Page 1, lines 4-11, as follows:

The present invention is related to the following commonly-assigned U. S. Patents, all of which were filed concurrently herewith: U. S. _____ (serial number 09/761,906 ~~09/_____~~), entitled "Secure Integrated Device with Secure, Dynamically-Selectable Capabilities"; U. S. _____ (serial number 09/764,844 ~~09/_____~~), entitled " Smart Card with Integrated Biometric Sensor"; U. S. _____ (serial number 09/761,899 ~~09/_____~~), entitled "Technique for Establishing Provable Chain of Evidence"; U. S. _____ (serial number 09/765,127 ~~09/_____~~), entitled "Technique for Improved Audio Compression"; and U. S. _____ (serial number 09/764,541 ~~09/_____~~), entitled "Technique for Digitally Notarizing a Collection of Data Streams".

Please amend the Abstract, as follows:

A method, system, computer program product, and method of doing business by improving security of a computing device. Continuous authentication of a user of the computing device, which may be (for example) a portable or personal computing device (also known as a "pervasive computing device"), is performed. ~~The disclosed techniques also improve the security of operations or transactions carried out with such computing devices.~~ Biometric sensors are preferably used for obtaining identifying information from users of computing devices, and this obtained information is compared to previously-stored biometric information which identifies the legitimate owner of the device. If the information matches, then it can be assumed that this user is the device owner, and a security-sensitive transaction is allowed to proceed so long as the biometric input is uninterrupted. Otherwise, when the obtained information does not match, or when there is an interruption in the biometric input, then the device may be in the wrongful possession of an impostor. A transaction may therefore be prevented or aborted, or in other cases perhaps simply marked as suspect or not authenticated; or, it may be desirable to completely deactivate the computing device.

Please amend the paragraph on Page 2 at lines 7-20 as follows:

Pervasive devices, sometimes referred to as pervasive computing devices, are becoming increasingly popular, and their functionality (in terms of communication and processing capabilities) is increasing rapidly as well. Pervasive devices are often quite

different from the devices an end-user might use in an office setting, such as a desktop computer. Typically, a pervasive device is small, lightweight, and may have a relatively limited amount of storage. Example devices include: pagers; cellular phones, which may optionally be enabled for communicating with the Internet or World Wide Web ("Web"); foreign language translation devices; electronic address book devices; wearable computing devices; devices mounted in a vehicle, such as an on-board navigation system; computing devices adapted to use in the home, such as an intelligent sensor built into a kitchen appliance; mobile computers; personal digital assistants, or "PDAs"; handheld computers such as the PALMPILOT™ brand handheld computer ~~PalmPilot™ from 3Com Corporation~~ and the WORKPAD® brand handheld computer ~~WorkPad®~~ from the International Business Machines Corporations ("IBM"); etc. (~~"PalmPilot"~~ "PALMPILOT" is a trademark of 3Com Corporation, and ~~"WorkPad"~~ "WORKPAD" is a registered trademark of IBM.)

Please amend the paragraph on Page 4 at lines 3-16 as follows:

Let us review the state of the prior art in the field of pervasive computing, as represented by a mobile professional equipped with a collection of the latest generation of specialized personal devices. She may have a cellular telephone, a two-way pager, a "smart" credit card (also known as a "smart card"), a "smart" employee badge used to access secure areas, a PDA, a digital still camera, a digital video camera, a dictation recorder with voice recognition capability, an MP3 music player, a remote control key-chain for access to an automobile, a second remote control key-chain for access to a garage, a global positioning system (GPS) navigation aid and map pad, a weather-alert radio, and a personal health alert fob to summon medical aid – all of which may be capable of interacting wirelessly with one another, perhaps via short-range radio technology such as Bluetooth. ("Bluetooth" is a standardized technology that enables devices containing a low-powered radio module to be automatically detected upon coming into radio proximity with one or more other similarly-equipped devices. Devices incorporating this technique are referred to as "Bluetooth-enabled" devices. A standard defining the Bluetooth techniques may be found on the Web at location www.bluetooth.com. ~~http://www.bluetooth.com.~~)

Please amend the paragraph beginning on Page 28 at line 18 and ending on Page 29 at line 14 as follows:

The security core now preferably computes a hash of this data block (Block 330). The security core then signs this hashed data block (Block 340) using the security core's private key. (The security core's private key is preferably securely stored in protected key storage, as shown at element 156 of Fig. 1 and as previously discussed.) Another data structure is then preferably created by the security core, where this data structure contains the original data block from Block 320 (shown as element 315) as well as the signed hash thereof which was computed in Blocks 330 and 340. This new data structure is then encoded (Block 350) as another data stream, referred to in this example as "S4", and this additional data stream is added to the collection as a notarization. In the preferred embodiments, the data streams S1 through S3 are SL-Packetized Streams within an MPEG-4 FlexMux stream, the timestamps T1 and T2 are encoded at the appropriate positions within the data streams S1 through S3 using MPEG-4 synchronization timestamp methodology, and the signed hash in stream S4 is an "n+1" MPEG SL-Packetized Stream that is also timestamped so that it can be correlated with streams S1 through S3. The notarized collection of data streams S1 through S4 may then be sent to a receiver, preferably as a FlexMux Stream over a TransMux Channel. (Alternatively, the notarized collection may simply be stored for future use.) An overview of the MPEG-4 standard, provided by the international standards working group responsible for its definition, can be found on the Internet at location www.cselt.it/mpeg/standards/mpeg-4/mpeg-4.htm. ~~http://www.cselt.it/mpeg/standards/mpeg-4/mpeg-4.htm.~~